A METHOD FOR USING A TELEPHONE CALLING CARD FOR BUSINESS TRANSACTIONS

Publication number: JP2002508547 (T)

Publication date: 2002-03-19

Inventor(s):

Applicant(s):

Classification:

- International: *G06Q20/00; G06Q30/00; H04M15/00; G06Q20/00;*
G06Q30/00; H04M15/00; (IPC1-7): G06F17/60; H04M15/00

- European: G06Q20/00K1; G06Q20/00K2B; G06Q20/00K3B; G06Q30/00C

Application number: JP20000538306T 19990322

Priority number(s): US19980079156P 19980324; WO1999US06195 19990322

Also published as:

WO9949404 (A1)

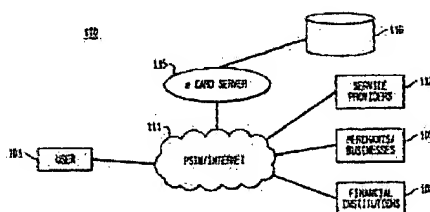ID28328 (A)

EP1064611 (A1)

CN1298526 (A)

CA2324114 (A1)

more >>

Abstract not available for JP 2002508547 (T)
Abstract of corresponding document: **WO 9949404 (A1)**

A method using a telephone calling card to transact commerce electronically. In one embodiment a user initiates a phone call to a merchant using a calling card provided by a service provider. The service provider initially checks the identify of the user through the use of a PIN code (1). Once the user's identity is validated the user's call to the merchant is established. The user and merchant then agree upon the sale of item at which time an invoice is provided to the service provider by the merchant. The invoice is then approved by the user while the merchant is disconnected from the call. In another embodiment the user is connected to the merchant over the Internet, the user's identify having been previously validated by an Internet Service Provider. The user drags a copy of the invoice to an application running on a Web Page. The application appends the user's digital signature to the invoice and mails it to the merchant. The merchant then presents the signed invoice to a server which authenticates the signature of the user prior to approving the sale.

Data supplied from the *espacenet* database — Worldwide

THE REQUESTED PATENT IMAGE IS NOT AVAILABLE FROM THE EPO WEBSITE.
BELOW IS THE ABSTRACT OF THE REQUESTED PATENT WHICH POSSIBLY LISTS
RELATED PATENT DOCUMENTS. IF YOU FEEL THIS MESSAGE IS IN ERROR, PLEASE
REATTEMPT DOWNLOADING THE PATENT OR DOUBLE-CHECK THE PATENT IMAGE
AVAILABILITY AT http://ep.espacenet.com.

ABSTRACT
A method using a telephone calling card to transact commerce electronically. In one embodiment a user initiates a phone call to a merchant using a calling card provided by a service provider. The service provider initially checks the identify of the user through the use of a PIN code (1). Once the user's identity is validated the user's call to the merchant is established. The user and merchant then agree upon the sale of item at which time an invoice is provided to the service provider by the merchant. The invoice is then approved by the user while the merchant is disconnected from the call. In another embodiment the user is connected to the merchant over the Internet, the user's identify having been previously validated by an Internet Service Provider. The user drags a copy of the invoice to an application running on a Web Page. The application appends the user's digital signature to the invoice and mails it to the merchant. The merchant then presents the signed invoice to a server which authenticates the signature of the user prior to approving the sale. <

CLAIMS
WHAT IS CLAIMED IS:
1. A method for electronic commerce using a trusted third party comprising the steps of:
a customer identifying himself to a network using a telephone calling card and the network completing a connection between the customer and a merchant;
negotiating, between the buyer and merchant, the terms for sale of an item selected by the customer;
signaling the trusted third party that the identified customer wishes to make a purchase;
forwarding, by the customer, a PIN to the trusted third party;
forwarding, by the merchant, an invoice having information on the selected item to the customer;
forwarding the invoice to a server for validation of the customer's approval and availability of funds;
securely signaling, by the customer, approval of the merchant's invoice; and
signaling, by the server, to the customer and the merchant approval of funds disbursement.

2. The method of claim 1 further comprising the step of billing the purchase to the customer's telephone or calling card bill.

3. The method of claim 2, wherein the step of customer identification comprises the steps of the user dialing a number for a telephone service provider, said dialed number having a PIN code uniquely associated with the customer, and the telephone service provider validating the identity of the customer based on the dialed PIN code.

4. The method of claim 3, where said customer signaling approval step comprises the substeps of:
the telephone service provider establishing two independent telephone calls, one call each to the customer and merchant;
the telephone system playing a recording of the merchant invoice for the customer; and
the telephone system collecting a keyed or spoken approval response from the user.

5. The method of claim 4, where the customer approval of an invoice comprises the substeps of the user obtaining a copy of the invoice and the user signing the invoice using a digital signature, created using either public or private key cryptography.

6. The method of claim 1, wherein the step of the customer identifing himself to the network comprises dialing into an Internet Service
Provider modem pool.

7. The method of claim 6, wherein the step of the customer identifying himself to the network further comprises the steps of the user using a computer to dial into said Internet Service Provider modem pool, inputting of a unique identification code by the user, and the Internet Service Provider validating the identity of the customer based on the inputted unique identification code.

8. The method of claim 7 where the step of the customer signaling approval of an invoice comprises the step of:
the customer placing a copy of the invoice into an eCard application running at the customer's computer;
the eCard application querying the customer for a password;
the eCard application creating a customer digital signature based on the password;
the eCard application appending the digital signature to the invoice;
the eCard application mailing a copy of said appended invoice to the merchant;
submitting, on the part of the merchant, of the signed invoice to an eCard server; and
validating, at the eCard server, the signature of the customer.

9. The method of claim 8, wherein said step of creating a customer digital signature is done using either public or private key cryptography.

DESCRIPTION
A METHOD FOR USING
A TELEPHONE CALLING CARD FOR BUSINESS TRANSACTIONS
FIELD OF THE INVENTION
The present invention relates to the field of commercialization for business transactions. More particularly, the present invention relates to the problem of securely and efficiently using a telephone calling card as a credit card for business transactions.

BACKGROUND OF THE INVENTION
More and more consumers are choosing to consummate purchases without physically entering the location where the service or item is located.

This social phenomena has grown in recent years due to the Internet, in particular the World Wide Web, and other electronically based shopping networks, such as the Home Shopping Network. In fact, virtual malls that allow consumers to wander from virtual store to virtual store through the use of a personal computer are available. In addition to home shopping, other areas that may ultimately be widely available via electronic commerce include movies on demand, video games, video libraries, home banking, and music on demand. It is particularly attractive to the consumer to purchase goods and services without the trouble of looking for a parking spot or waiting in line.

Indeed, electronic commerce could one day be the dominant means used for purchasing any and all items or services and may very well revolutionize the way business is conducted.

In today's economy, a consumer wishing to make a modest electronic purchase (i. e., without being physically present) has only two alternatives. If he is conducting business through the computer, he can use some secure electronic payment scheme, such as eCash or MilliCent. Otherwise, the only instrument

available is the ordinary credit card.

eCash is a software-based payment system that allows users to make electronic payments from any computer to any other computer over any computer network including the Internet. An eCash purchase requires three participants-a buyer, a seller, and a bank. Initially, the buyer withdraws digital coins, or eCash, from her bank account. The digital coins are in fact messages having strings of digits with each digital string corresponding to a different digital coin. The messages are transmitted to the buyer's computer where eCash software automatically manages the digital coins. A buyer having eCash on hand may then make purchases from a seller or merchant who has previously signed up to the eCash transaction system. Before a sale is consummated between buyer and seller, however, the seller's software automatically sends the digital coins it receives from the buyer to the bank.

By sending the coins to the bank the seller is able to protect herself against fraud. As such, the bank is used as a central authority. In order to protect the privacy of the buyer eCash uses"blind signatures", as described in Chaum,

David L., U. S. Patent No. 4,759,063, entitled"Blind Signature Systems", and

Chaum, David L., U. S. Patent No. 4,949,380, entitled"Retumed-Value Blind

Signature Systems". One drawback of this system is that in order to make a purchase both the buyer and the seller must have accounts on the eCash system. This drawback may be particularly chilling in that the impulse to buy an item or service may not survive the time it takes for a consumer to sign up with such a system. Another drawback is that each purchase requires processing by an intermediary, e. g., a bank, before the purchase is deemed completed.

MilliCent is another software based payment system primarily designed for content-based Internet commerce. The MilliCent system is based on the use of"scrip". Scrip is a pre-paid electronic coupon that essentially replaces cash for purchases. Scrip is issued by brokers, that act as intermediaries between consumers and vendors, or by vendors. Basically, a consumer, by way of a credit card, for example, buys vendor specific scrip, i. e., that scrip can only be used to purchase content from a particular vendor, either from a broker or vendor, and then uses the scrip to make purchases. While the MilliCent system does not require user accounts it also has drawbacks. For one, each user must subscribe and use MilliCent software. In addition, scrip is vendor specific thereby limiting the flexibility of the shopping consumer.

Thus, not unlike eCash MilliCent may have a negative impact on the spur of the moment purchase. On the other hand, the low transactional costs associated with systems such as eCash or MilliCent make them particularly attractive for purchasing items or services that cost as little as 10 cents. eCash and MilliCent are just two of the many prior art schemes that provide for secure electronic commercial transactions over computer networks. Other popular schemes include CyberCash, NetBill, NetCash and NetCheck, and systems offered by Netscape, First Virtual Holding, and NTT.

Despite the variety of these electronic commerce systems, these systems share a common goal of providing a system that is secure against fraud, security breaches, or counterfeiting, and assures consumer privacy. In order to provide an adequate measure of security almost all electronic commerce systems employ encryption techniques. As such, both public key and private key encryption or decryption schemes are used to establish the identity of the buyer or the merchant, to verify information, and to provide electronic signatures that are legally binding and not likely to be forged.

Consumers who use credit cards to remotely shop are afforded greater flexibility in choosing with whom they transact business than are consumers who use electronic commerce systems such as eCash or MilliCent. A consumer using a credit card to make an electronic purchase first requests the purchase from the merchant. The merchant then contacts the institution that issued the consumer's credit card for authorization. If the purchase is authorized, the merchant is eventually given a token which the merchant

transfers into its bank account and the consumer is forwarded a bill from the institution. Using a credit card to make an electronic purchase has it own set of problems. First, although encryption is used in credit card transactions to protect information such as credit card numbers, credit card security is poor.

Any merchant can take the information given by the user and purchase addition goods from other merchants; even if the fraud is detected, there is little hope of tracing it back to the dishonest merchant. The danger of eavesdropping or snooping by an outsider to the transaction also poses a significant risk. More significant is the risk associated with break-ins at a host where credit card numbers may be stored. Second, and probably more importantly, credit card overheads are typically high ($0.20 + 2% of transaction cost is typical). This makes credit card payment inappropriate for payments under $1.00.

Of utility then would be a method and system that allows a consumer to purchase items or services from merchants without requiring either the merchant or consumer to install proprietary software. In addition, such a system or method should be secure by not requiring the consumer to divulge private information, such as credit card numbers, that may be misappropriated. Finally, such a system should be ubiquitous allowing any and all consumers to make purchasers without visiting a store.

SUMMARY OF THE INVENTION
Our invention is a method and system that uses a telephone card to make payments as part of an electronic commercial transaction.

Our system includes an eCard server connected to a public network through which a consumer and a merchant can communicate and transact business. In accordance with our system, the public network may be the
Internet or the Public Switched Telephone Network (PSTN). Accordingly, our system provides the opportunity for in-home shopping without requiring the consumer to own a personal computer or a credit card.

In conducting purchases over the Internet in accordance with our invention, a secret encryption key is shared by the user and the calling card server. In general, when a user or consumer wishes to make a purchase, he contacts the merchant, who prepares an invoice. The user signs the invoice using his telephone calling card number and a PIN code. The merchant then sends the signed invoice to the eCard server. The server authenticates the signature, verifies that the user has sufficient funds for the purchase, and sends a confirmation to the merchant. After receiving confirmation the merchant then informs the user of the successful purchase. The user is later billed for the item on his phone bill, and the invoice is preserved at the eCard server for auditing and to guarantee non-repudiation of the transaction. In accordance with our invention no private information is passed on to the merchant (even the customer name can be hidden). As such, the risk of fraud is reduced.

In accordance with an embodiment of our invention purchases may be conducted over the PSTN. In accordance with this embodiment the user first initiates a phone call to the merchant using his telephone calling card. Thus, the user first identifies himself to the telephone network. The telephone network then completes the call to the merchant so that the merchant and the user can negotiate a transaction. Once negotiations are completed either the user or the merchant signals the telephone system to mediate a transaction; for example, the user may use a flash-hook/dialed code, or the merchant may use the Internet. The merchant transfers an audible invoice along with the user's PIN (so the user can authenticate the purchase is actually being made) to the eCard server. The eCard server then plays the audible invoice and the user's pin to the user so that the user can agree to either accept or decline the purchase. If the purchase is agreed to, the user is billed for the item on a subsequent telephone phone bill, and the invoice is again saved for future auditing and non-repudiation. A further extension of this embodiment of our invention includes the user purchasing a prepaid calling card, thereby removing the

addition step of later billing the user.

In accordance with another embodiment of our invention transactions may occur via the Internet using the World Wide Web. In this embodiment, the consumer first dials into a server maintained by an Internet Service
Provider (ISP), which can be a telephone company. As part of the dial in process the consumer's identity is validated. The user then drags a copy of an invoice or purchase order to an application running on a Web Page. The application appends the user's digital signature to the invoice and mails it to the merchant. The merchant then presents the signed invoice to the eCard server which authenticates the signature of the user prior to approving the sale.

Our invention affords several advantages over the prior art. Some of these advantages include:
The widespread availability of calling cards provides more sales
opportunities for merchants. Because calling cards are even more
widely available than credit cards, a much large segment of the
purchasing public are therefore available to merchants as potential
electronic commerce customers. More importantly these customers
need not be credit worthy as customers may purchase pre-paid cards
having different levels of digital money available;
Even where billing is necessary practically every telephone
customer is already being billed on a monthly basis, making the billing
overhead smaller;
Calling cards, unlike most credit cards, are secured (with the
customer's utility service). Because the telephone service provider has
greater leverage than a typical bank, it is less likely to have to spend
large amounts of money on collections;
The calling card infrastructure is designed to handle much
smaller payments than the financial services infrastructure;
Telephone companies can leverage the security available from
the existing PSTN to provide better security and user authentication;
Telephone companies are generally trusted by both the public
and merchants, and so they can serve as a suitable"trusted third party"
in contract protocols; and
User identity can be kept private for those transactions that do
not involve shipping (e. g., paying for downloaded maps or videos).

Additional objects, advantages and novel features of the invention will be set forth in the description which follows and, in part, will become more apparent to those skilled in the art upon examination of the following or may be learned by practice of the invention. The objects and advantages of the invention may be realized and attained by means of the instrumentalities and combinations particularly pointed out in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS
FIG. 1 illustratively depicts the system architecture of the present invention.

FIG. 2 is a state diagram depicting the information flow between the elements depicted in FIG. 1 in carrying out a transaction over the PSTN; and
FIG. 3 is a state diagram depicting the information flow between the elements depicted in FIG. 1 in carrying out a transaction over the Internet.

DETAILED DESCRIPTION OF THE INVENTION

Turning to FIG. 1 there is depicted a generalized schematic of a system 100 in accordance with our invention. The system 100 connects users or consumers 101 to various merchants or businesses 105 and financial institutions 106 through either the Public Switched Telephone Network or
Internet 111. The user's 101 connection to merchant 105 is established or managed by a service provider or a trusted third party 112, i. e., an Internet
Service Provider (ISP) or a telephone company. A calling card or eCard server 115 is also connected to the network 111 and stores a list (illustratively depicted as database 116) of calling card numbers, PINs, user names and addresses, and credit limits, if any. It should be noted that although we illustratively separate the merchant 105 from the service provider 112 the merchant and service provider might be the same entity. For example, some telephone companies already have their own on-line shopping networks. In general, after service provider 112 connects the user 101 to merchant 105, the user 101 initiates operation of the system by selecting an item or service offered by merchant. Once a price is negotiated between the user 101 and the merchant 105, the user 101 selects the eCard as the method of payment.

Once the method of payment is selected, a series of actions, discussed in detail below, are initiated and managed by eCard server 115, which actions allows the user 101 to be billed for the service or good.

Calling cards are issued by all major telephone companies. These cards have proven to be an effective and convenient way for customers to make toll calls when away from home. Typically, the user dials a toll-free number and types his calling card number and a secret code (PIN). The service provider checks the validity of the number and correctness of the PIN and allows the user to place toll calls. Charges for the calls appear on the user's telephone bill. As such, calling cards already provide a secure method of connecting users over the PSTN. Our invention leverages the security already present in the PSTN and enhances this security on computer networks, e. g., Internet, by using cryptographic techniques.

The primary cryptographic technique used in our invention is private digital signatures. To use these signatures, the user 101 and the server 115 share a secret key. In order to sign a document, the user 101 appends the secret key to the document and computes a cryptographic checksum, using a standard cryptographic hash function such as MD5 or SHA. The checksum is sent along with the document to the server 115, which performs the same checksumming process. If the checksums agree, the server 115 can be sure that document was signed by the user 101. A private digital signature is the preferred encryption method because each telephone calling card customer can be given a private key at the time the card is disbursed. Private key encryption is also better suited for our invention because here there is no arbitrary person to whom consumers must identify themselves. More importantly, private key encryption is cheaper to implement and takes advantage of the fact that the service provider issues calling cards and serves as the trusted third party. Nonetheless, public key cryptographic techniques may also be used to authenticate the signature of the customer.

Turning now to FIG 2., there is illustrated the method steps of a first embodiment of our invention which allows a consumer to make a purchase over the PSTN. As FIG. 2 shows the process begins when a consumer or customer 101 places a telephone call 202 to a merchant 105 from either the consumer's home, or by using a calling card, or through some other mechanism identifies himself to the PSTN. Once the consumer's identity is established, the consumer's service provider system or PSTN 11 establishes the call 202 between the consumer 101 and the merchant 105. The consumer 101 and merchant 105 then negotiate a transaction 208.

Once negotiations are completed the consumer 101 hits a predetermined sequence of keys 210 on the telephone pad, e. g., flash hook followed by *678, to signal the service provider system 111 that a consumer wishes to make a purchase. When the service provider system 111 receives this sequence or signal 210 the system 111 temporarily disconnects both the merchant 105 and the consumer 101 and establishes two new calls, one 212 to the consumer 101 and the other 214 to the merchant 105.

Alternatively, instead of temporarily disconnecting the merchant 105 and consumer 101 the system may alternate temporarily disconnecting the merchant 105 and the consumer 101 from the call. If the consumer is using a calling card, the consumer is queried for his PIN, step 216. Of course, if the consumer is calling from home a PIN may not be necessary. While the customer is queried for his PIN, step 216, the merchant is also queried to enter the transaction amount, step 218. The consumer and merchant then each return the information requested, steps 220 and 222, respectively. In returning the information requested both the consumer and the merchant may also be requested or allowed to return additional information pertaining to the transaction. For example, the consumer may input his name and address, step 224, and have this information recorded by the service provider 111.

Likewise, the merchant may input its name and the items purchased, step 226, and have this information recorded by the service provider 111. This addition information provided by the merchant may be disclosed to the consumer or vice versa. Furthermore, the merchant may forward the information by way of an audible invoice or an invoice on the Internet to the service provider. However, the addition information is not needed to consummate the sale. This is the case because both parties to the transaction already know the item selected and the price.

The service provider then checks the consumer and merchant records to select an appropriate form of payment and the availability of funds on the part of the consumer, step 227. As illustrated by FIG. 2, step 227 involves the service provider accessing the eCard server 115. It should be noted that although in the above description the service provider system 111 is described as collecting information from the consumer and the merchant, the service provider system 111 may also function as traffic cop allowing the eCard server 115 to request, collect, and manage the entire transaction.

Once the method of payment is selected the service provider plays the product description and price to the consumer, step 230, and receives confirmation from the consumer, step 232. Once confirmation is received the consumer and merchant are then reconnected, step 235.

In a second embodiment of our invention, and as illustrated in FIG. 3, the consumer may also purchase items over the Internet using an application available on the World Wide Web (Web). The consumer begins the transaction by dialing into an Internet Service Provider (ISP) modem pool, inputting a user identification code and password, step 302. The ISP then validates the user and establishes a connection to a Web page from which the customer negotiates an item and price, step 304. The consumer then clicks on a eCard icon, step 306, on the Web page used to negotiate the transaction; note that the Web page may be the Web page of the consumer or some other trusted third party. As a result two new connections are created, one from the consumer to the eCard server, connection 308, and one from the eCard server to the merchant, step 310. The eCard server then queries the consumer for his calling card PIN, step 312. At the same time, the merchant is requested to enter the amount of the transaction on an invoice or purchase order 314. As was the case in the previous embodiment of our invention, the consumer and merchant may optionally record a message indicating any other specific terms related to the transaction, steps 318 and 320, respectively. Using voice, a Web page, or off-line email the service provider system may optionally play a recording of the customer's voice and name. The system then checks the customer and merchant records, step 330, to select an appropriate form of payment (typically on the calling card account, but possibly on a credit card, ATM, etc.). The system then confirms to the customer, step 336, the product description and price and also receives confirmation from the customer, step 338. After customer confirmation, step 338, the consumer is again free to roam the Web and make another purchase.

The above description has been presented only to illustrate and describe the invention. It is not intended to be exhaustive or to limit the invention to any precise form disclosed. Many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in

order to best explain the principles of the invention and its practical application to enable others skilled in the art to best utilize the invention on various embodiments and with various modifications as are suited to the particular use contemplated.